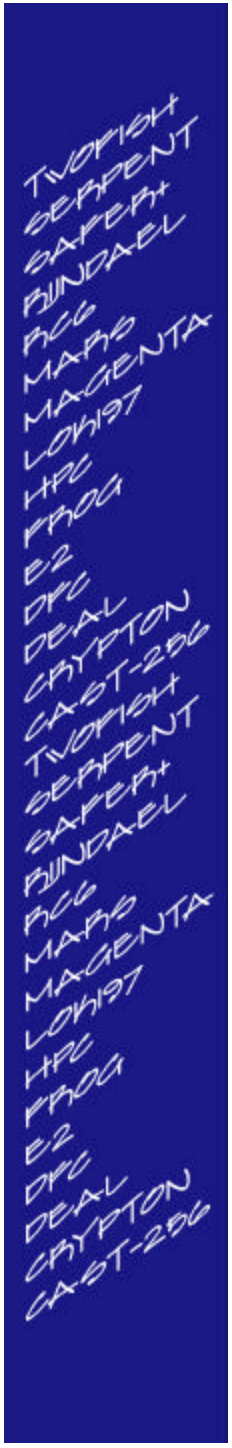


WELCOME!

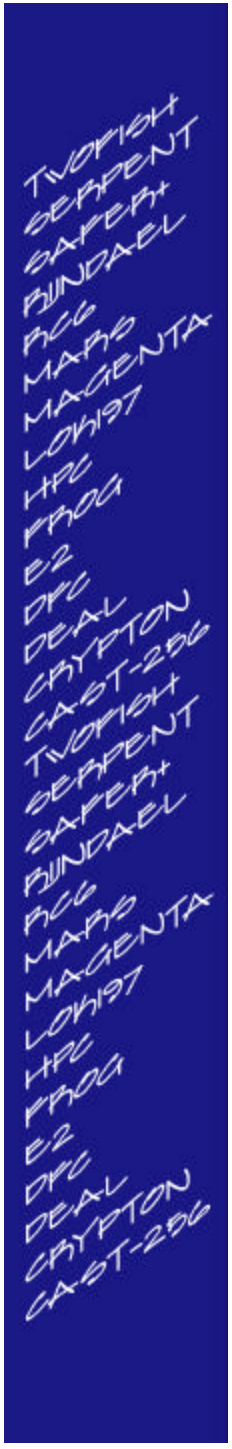
The First Advanced Encryption Standard (AES) Candidate Conference

August 20-22, 1998

Double Tree Hotel

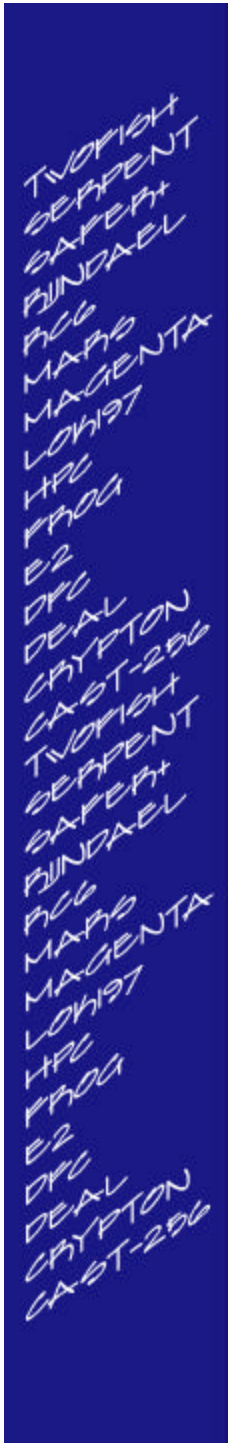
Ventura, California

“It’s time for those 128-, 192-, and 256-bit keys”



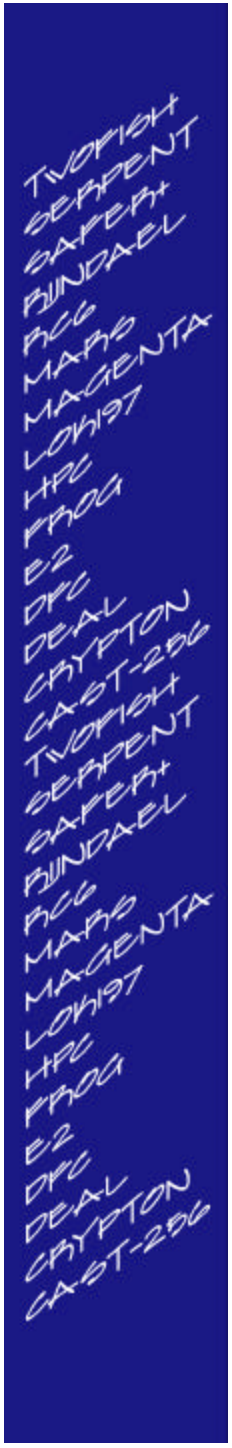
AES1 Conference Overview

- Formal presentation of candidate algorithms and design philosophies
- Distribution of CD-1: Documentation
- Call for analysis
- Discussion
- Announcement of Second AES Conference



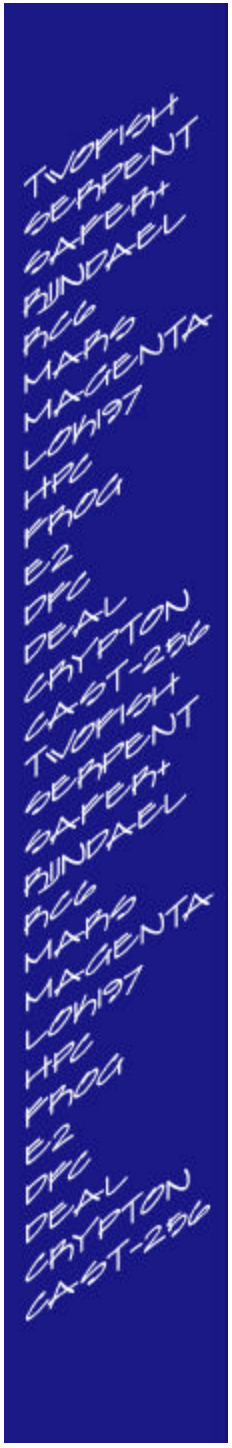
Logistics

- Presentations: 30-35 minutes
- Questions: 10 minutes
- Sessions to start when scheduled
- Discussion at end of each day
- Breaks and Lunch
- For assistance Ms. Vickie Harris



What has been done so far?

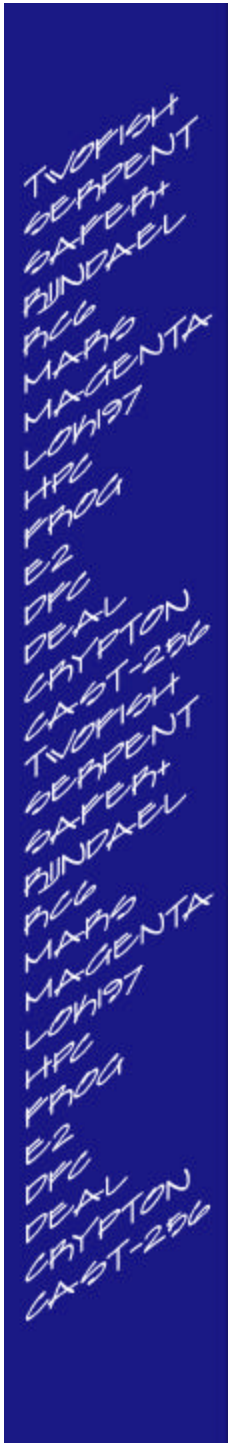
- Announcement of intent to develop AES and request for comments, January 2, 1997
- Workshop on proposed requirements and procedures, summary of comments, April 15, 1997
- Informal draft requirements and procedures, June 16, 1997
- Formal call for candidate algorithms, Sep. 12, 1997
- Submission for pre-review, April 15, 1998
- Results of pre-review, May 15, 1998
- Close of call, June 15, 1998
- Notification to submitters, July, 1998



Selecting the Candidates

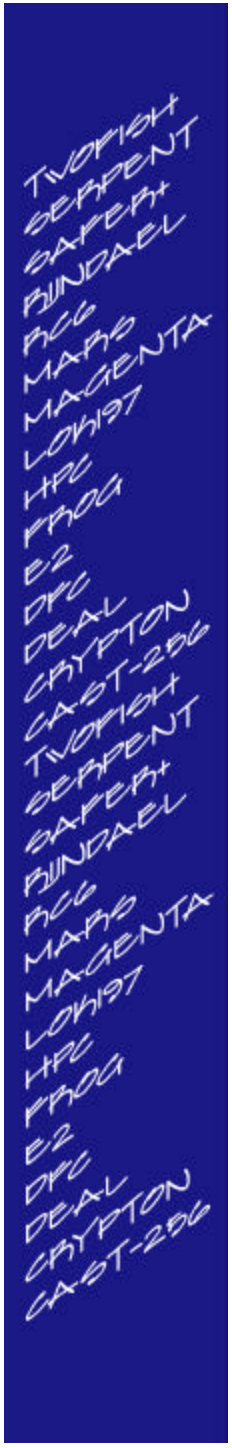
- Twenty-one packages received
- NIST verified that legal documents were completed
- NIST verified that responses were provided for all items
- NIST attempted to run code and verify Known Answer Tests
- Six packages found to be incomplete
- No cryptanalysis performed

TWOFISH
SERPENT
SAFER+
BLOWFISH
RC6
MARS
MAGENTA
LOKI97
HPC
FROG
E2
DFC
DEAL
CRYPTON
CAST-256
TWOFISH
SERPENT
SAFER+
BLOWFISH
RC6
MARS
MAGENTA
LOKI97
HPC
FROG
E2
DFC
DEAL
CRYPTON
CAST-256



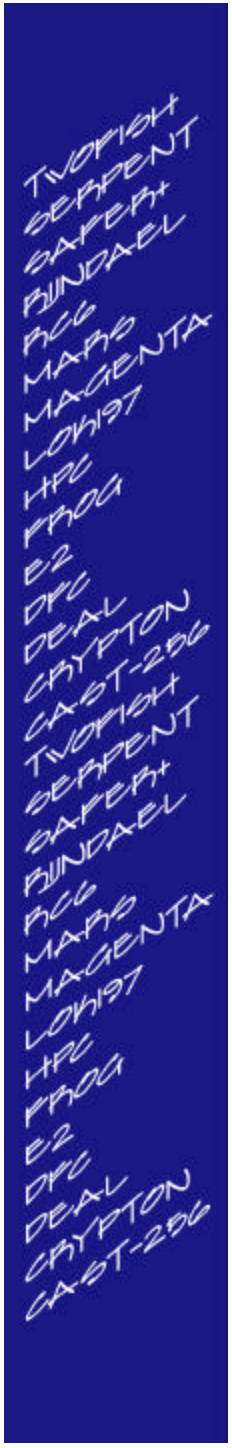
Candidate Algorithms

- **Australia**
  - LOKI97 — Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
- **Belgium**
  - RIJNDAEL — Joan Daemen, Vincent Rijmen
- **Canada**
  - CAST-256 — Entrust Technologies, Inc.
  - DEAL — Outerbridge, Knudsen
- **Costa Rica**
  - FROG — TecApro Internacional S.A.
- **France**
  - DFC — Centre National pour la Recherche Scientifique (CNRS)
- **Germany**
  - MAGENTA — Deutsche Telekom AG



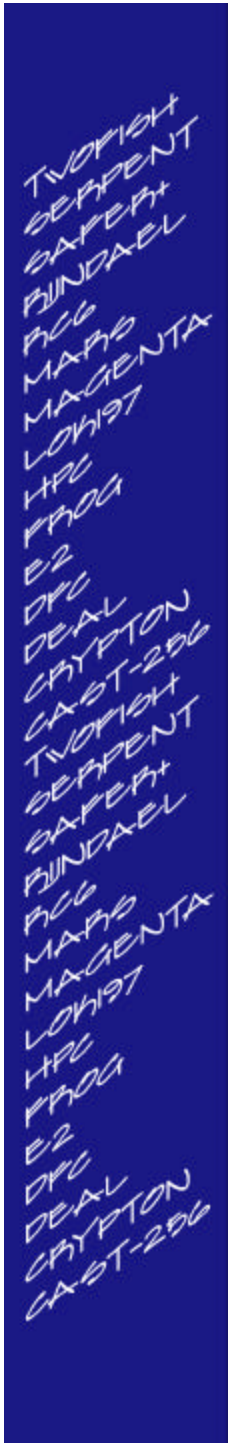
Candidate Algorithms, cont'd

- **Japan**
  - E2 — Nippon Telegraph and Telephone Corporation (NTT)
- **Korea**
  - CRYPTON — Future Systems, Inc.
- **USA**
  - HPC — Rich Schroeppel
  - MARS — IBM
  - RC6 — RSA Laboratories
  - SAFER+ — Cylink Corporation
  - TWOFISH — Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
- **UK, Israel, Norway**
  - SERPENT — Ross Anderson, Eli Biham, Lars Knudsen



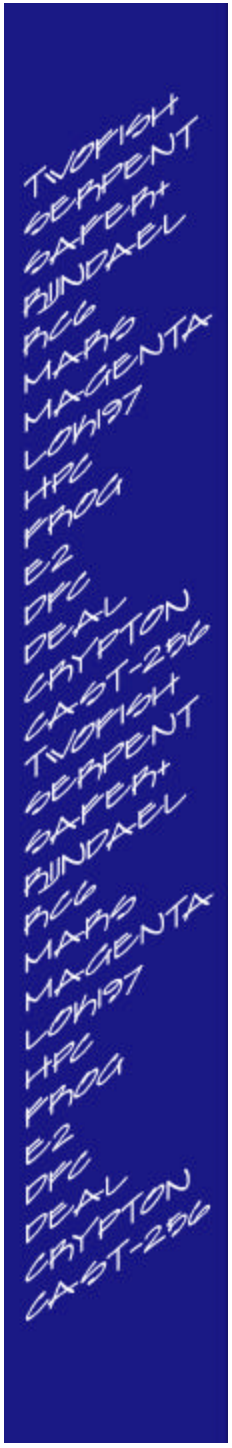
What are we looking for?

- Very strong symmetric block cipher for government and commercial use in the next century
- More efficient than Triple DES
- More secure than Triple DES
  - Key sizes: 128, 192, and 256 bits
  - Block sizes: 128 bits (other sizes optional)
- Publicly defined and evaluated
- Worldwide royalty free



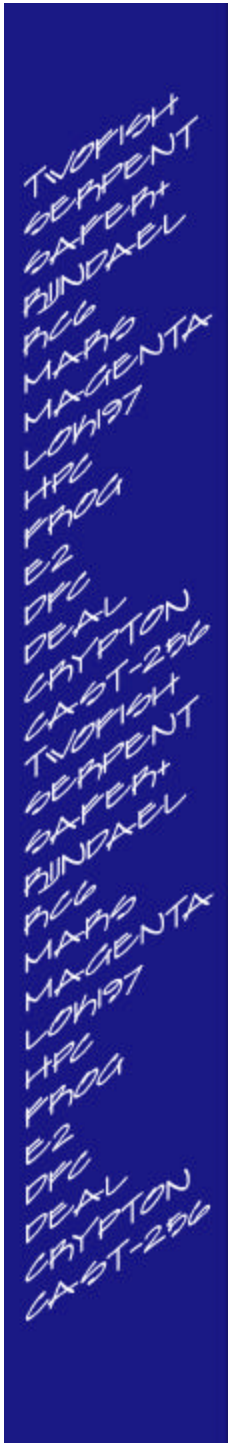
Next Steps

- Public review of candidates, Aug. 20 - April 15, 1999
- Submissions of analysis for AES2, Feb 1, 1999
- Second AES conference
- Submissions of analysis for Round 1, April 15, 1999
- Announcement of (about) five finalists
- Public Review of finalists, 6-9 months
- Third AES Conference
- Selection of AES Algorithm
- Make AES a FIPS



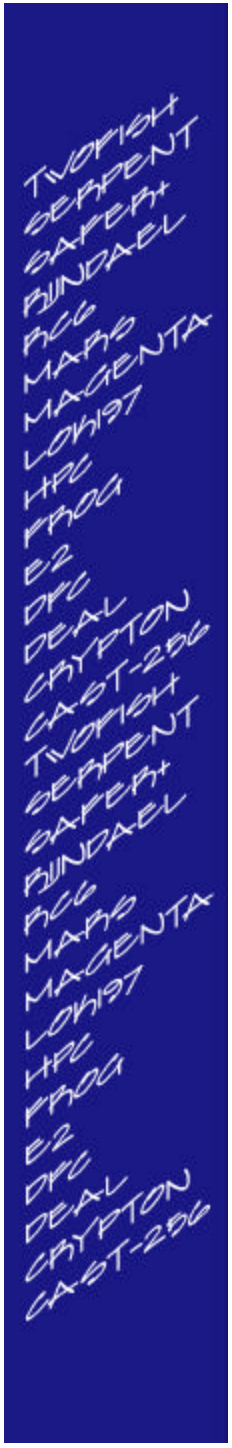
1

Review of AES Evaluation Criteria



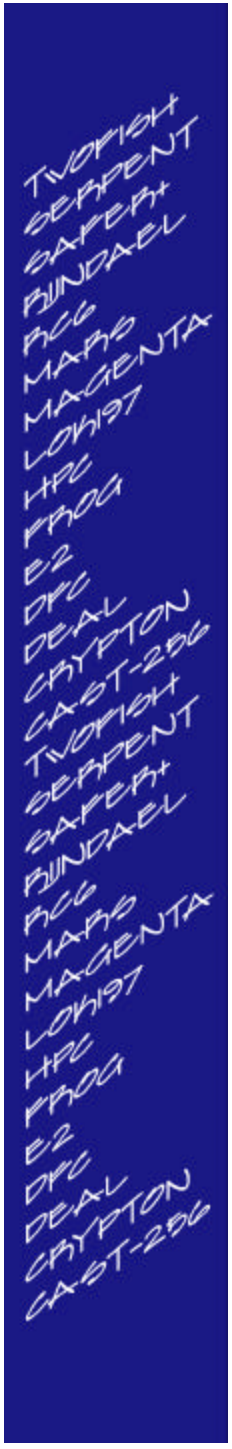
Evaluation Criteria

- Categories:
  - Security
  - Cost
  - Algorithm and Implementation Characteristics



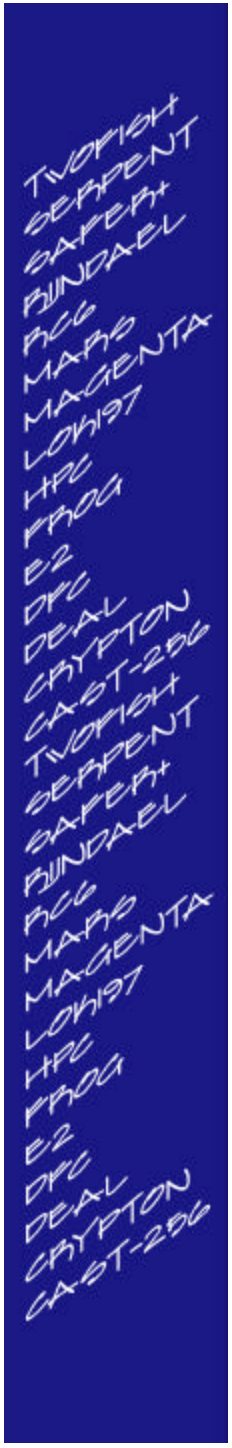
Security

- *Paramount consideration*
- Security compared to other candidates
- Extent to which the algorithm output is indistinguishable from a random permutation on the input block
- Other security factors, particularly singling out attacks that demonstrate that the actual security of the algorithm is less than the strength claimed



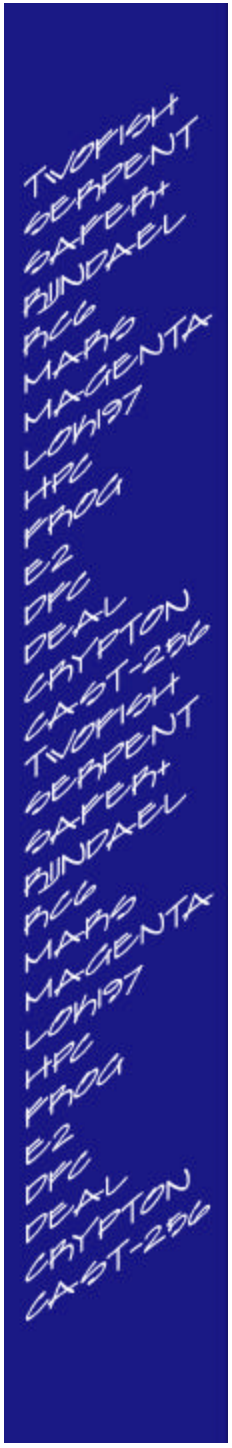
Cost

- Licensing requirements
  - royalty-free (if selected) worldwide
- Computational efficiency (speed)
  - not limited to NIST test platform tests
  - R1 focus 128-128 (but not exclusively)
  - R2 focus expanded to 192-256 & h/w
- Memory requirements
  - e.g., code size, memory requirements, etc.



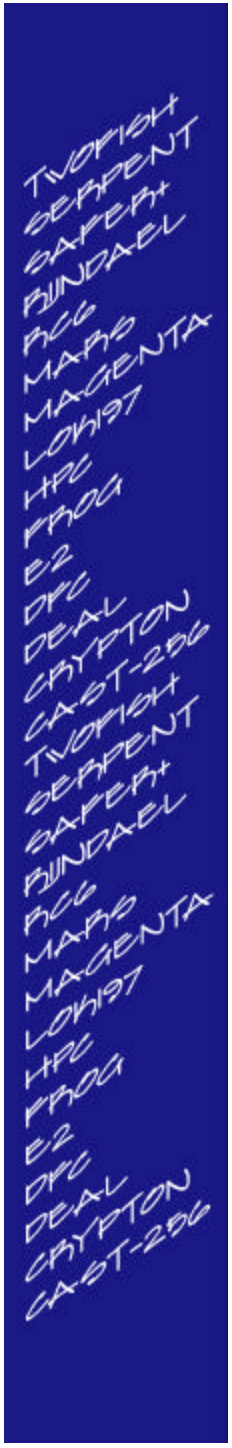
Algorithm and Implementation Characteristics

- Flexibility
  - e.g., key and block sizes supported
  - suitability for implementation in a wide variety of platforms / applications
    - e.g., 8-bit processor smart cards
  - use for other purposes,
    - e.g., stream cipher, MAC, pRNG, hash



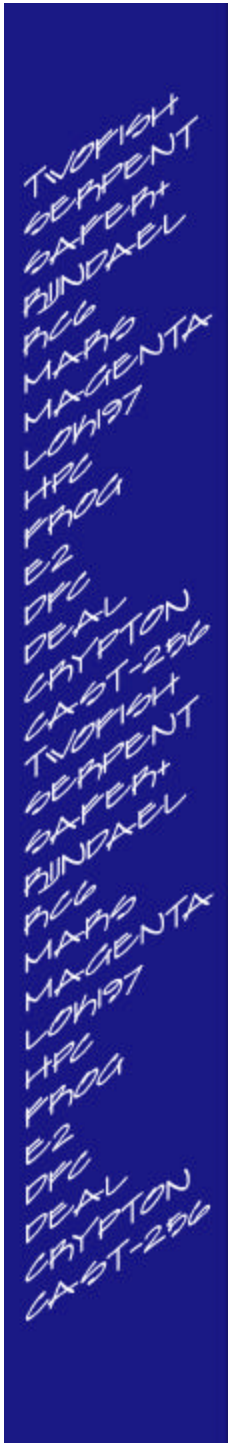
Algorithm and Implementation Characteristics

- Hardware and software suitability
  - any special issues?
- Simplicity



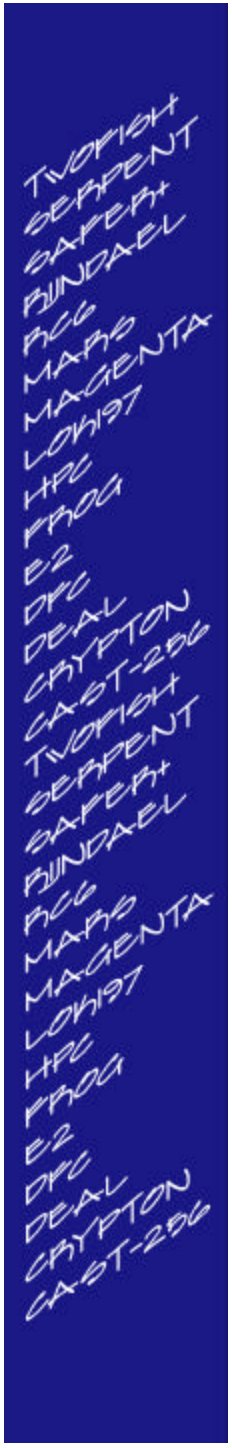
2

Facilitating Discussion of AES Candidate Algorithms



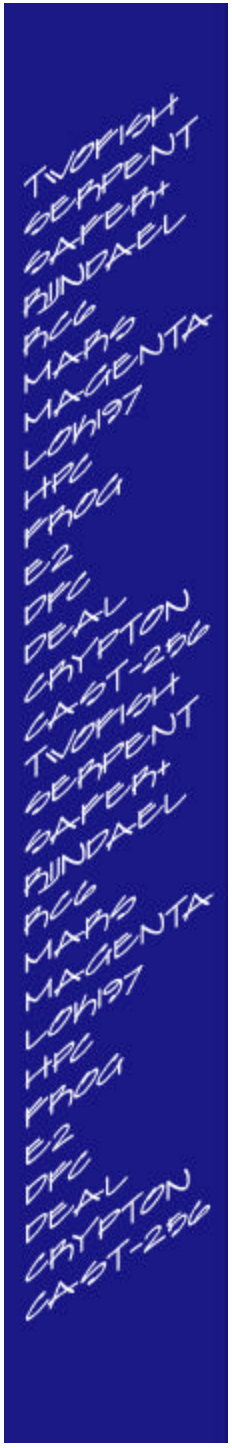
Facilitating Discussion of AES Candidates

- NIST is establishing a discussion group at www.nist.gov/aes for each candidate
- Intended to aid interaction among parties interested in particular algorithm(s)
- Provides a focal point for submitters to monitor discussion of their candidates
- Submitters may participate (encouraged!), at their discretion



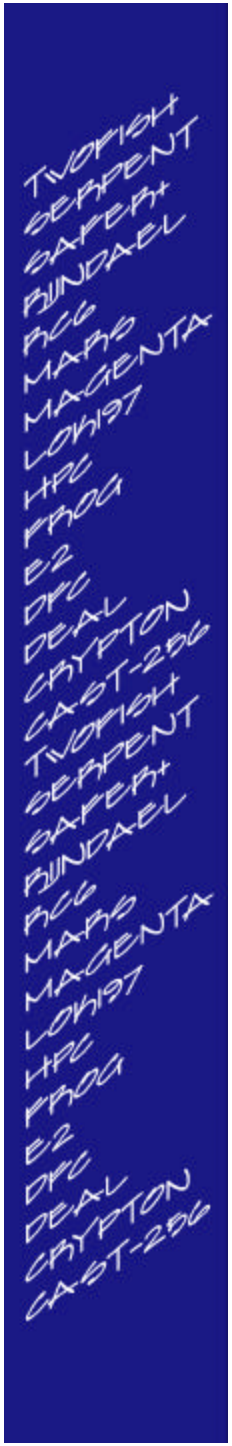
Facilitating Discussion of AES Candidates

- NIST welcomes suggestions about these groups, and topical ideas for other AES-related discussions
  - (e.g., general intellectual property, time schedule, plans for second conference, etc.)
- All discussion postings will be publicly available but not part of the *formal* public record
  - allows give-and-take before submitting a formal recommendation to NIST



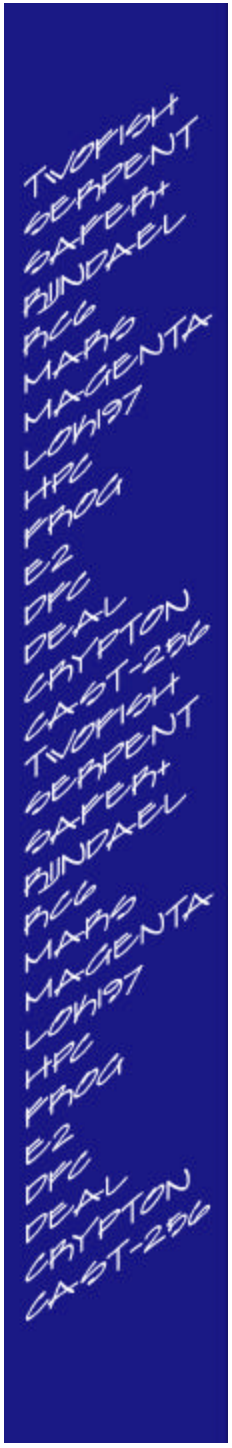
3

Submission of Formal AES Comments



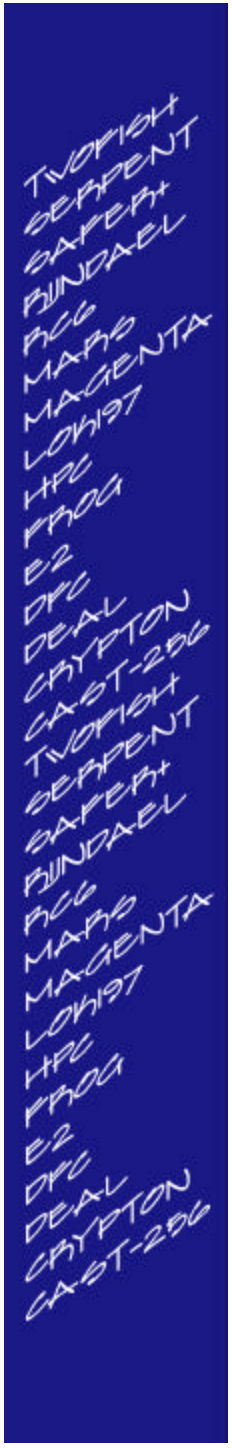
Submitting Formal Comments to NIST

- As part of FIPS development, NIST collects formal public comments
- Submitters may also, of course, submit comments
- Comments are publicly available
- E-comments, at a minimum, will be available at www.nist.gov/aes after close of comment period
- e-mail: `AESFirstRound@nist.gov`



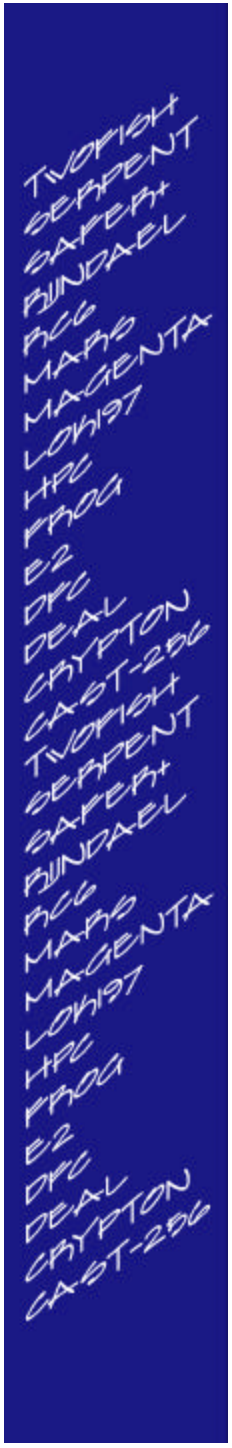
What sort of comments?

- NIST seeks comments on all aspects of the candidates
  - regarding specific algorithms and any aspect of the evaluation criteria
  - regarding intellectual property
    - specifically about any other patents
  - cross-cutting analysis
  - overall recommendation



Comment Deadlines

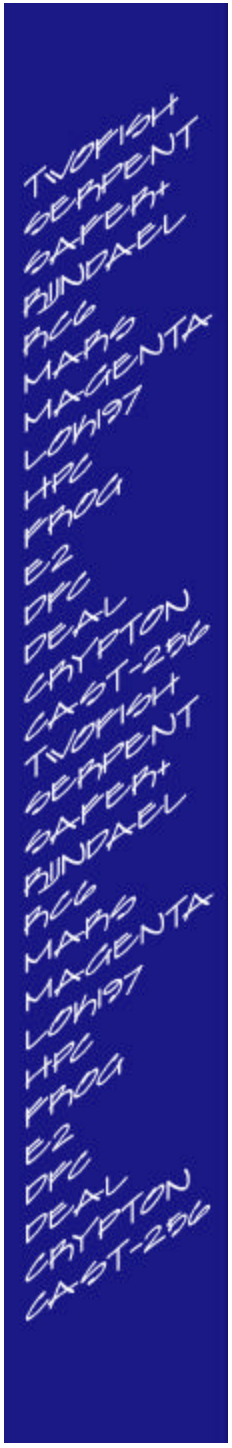
- Best of the comments / analysis submitted will be considered to be invited to brief at the Second AES Candidate Conference
- To allow sufficient time for agenda planning, *for consideration for second conference*, comments must be received by 2/1/99
- All comments for R1 due 4/15/99
  - allows for submission of comments based upon results of Second conference



NIST requests ...

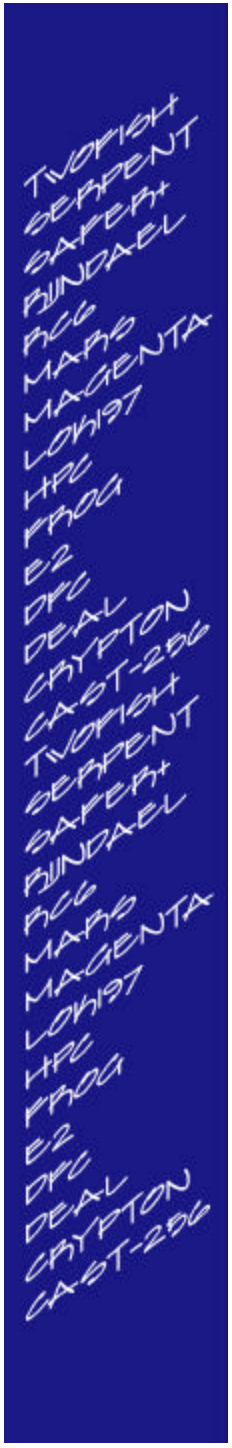
- It would help NIST if
  - your comments are very clear as to which algorithms your comments apply
  - if you can recommend a "final five" *with justification*

- *Note that NIST does not respond directly to comments. NIST analyzes and uses them as input for the next step in AES process.*



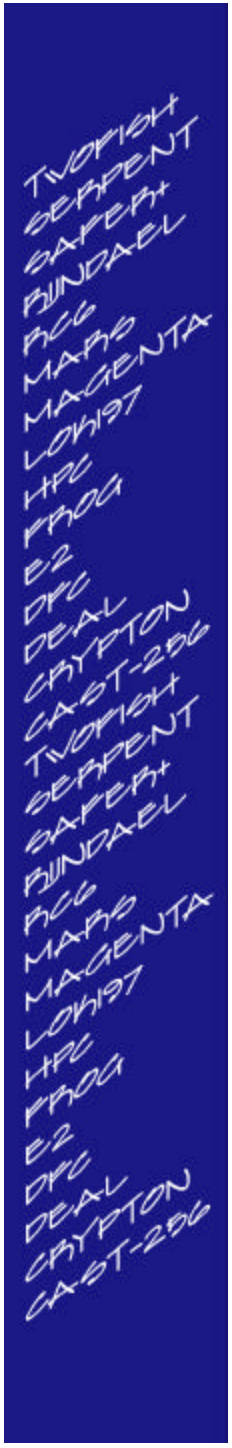
4

NIST's AES Efficiency Testing Plans



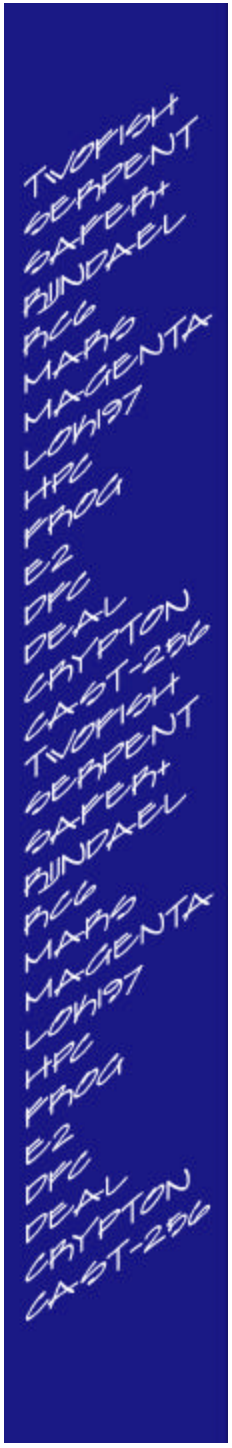
NIST's testing

- Will measure efficiency of Java™ and ANSI C (optimized) implementations
- Platform: IBM-compatible PC/ Intel Pentium-pro Processor 200MHz, 64MB RAM
- Other platforms, time / resources permitting
- Planning to test output for randomness



Measurements

- Algorithm setup
- Key setup
- Key change
- Encrypt
- Decrypt



V.I.N.

(Very Important Note)

The purpose of NIST conducting these tests is to ensure at least one set of efficiency measures of the entire field of candidate algorithms is conducted.

Other such measurements, on different platforms, including in different computer languages, is most welcome!